대한민국특허청
KOREAN INTELLECTUAL PROPERTY OFFICE

별첨 사본은 아래 출원의 원본과 동일함을 증명함.

This is to certify that the following application annexed hereto is a true copy from the records of the Korean Intellectual Property Office.

출 원 번 호 : 10-2002-0064702
Application Number

출 원 년 월 일 : 2002년 10월 22일
Date of Application OCT 22, 2002

출 원 인 : 최운호
Applicant(s) CHOI UN HO

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

2003 년 10 월 21 일

특 허 청
COMMISSIONER

【서지사항】

【서류명】	특허출원서
【권리구분】	특허
【수신처】	특허청장
【제출일자】	2002.10.22
【발명의 명칭】	ＩＳＡＣ 형태의 전사적 종합 침해사고 대응시스템 및 방법
【발명의 영문명칭】	ISAC(Information Sharing and Analysis Center System) and CERT(Computer Emergency Response Team) of Information Security and Management Method Thereof
【출원인】	
【성명】	최운호
【출원인코드】	4-2002-035919-2
【대리인】	
【성명】	이철희
【대리인코드】	9-1998-000480-5
【포괄위임등록번호】	2002-073160-2
【대리인】	
【성명】	송해모
【대리인코드】	9-2002-000179-4
【포괄위임등록번호】	2002-073161-0
【발명자】	
【성명】	최운호
【출원인코드】	4-2002-035919-2
【취지】	특허법 제42조의 규정에 의하여 위와 같이 출원합니다. 대리인 이철희 (인) 대리인 송해모 (인)

【수수료】

【기본출원료】	20 면	29,000 원
【가산출원료】	22 면	22,000 원
【우선권주장료】	0 건	0 원
【심사청구료】	0 항	0 원
【합계】	51,000 원	
【감면사유】	개인 (70%감면)	
【감면후 수수료】	15,300 원	

출력 일자: 2003/10/28

【첨부서류】

1. 요약서·명세서(도면)_1통

【요약서】

【요약】

본 발명은 개인이나 민간의 IT 정보, 회사의 정보 등을 네트웍이나 정보 기반 구조(Information Infrastructure)의 기술로 이루어진 원격지에서 시스템 상호 간에 데이터를 공유함과 더불어 해킹이나 사이버 테러 등의 비인가된 접속을 차단하여 침해 사고에 종합적으로 대응할 수 있도록 구성된 ISAC/CERT 형태의 전사적 종합 침해사고 대응시스템(ESM:Enterprise Security Management) 및 방법에 관한 것이다.

본 발명에 따른 전사적 종합 침해사고 대응 시스템(ISAC: 200)은 CERT 운영 시스템부(210), 조기 경보부(212), 사이버테러 공격평가부(214), 사고 접수부(216), 사고접수 데이터베이스(218), 종합상황 디스플레이부(220), ESM 관리 시스템부(230), 컴퓨터 포렌식 데이터베이스(232), 취약성 데이터베이스(234), 소스/가공 데이터베이스(236), 테스트베드(238), 시스템 점검부(240), 보안 프로그램부(250), 보안장치 관리부(260), 인식장치 관리부(270) 등을 포함한다.

본 발명에 의하면, 자동화되고 체계적인 해킹/사이버테러 등 침해 사고 대응 체계를 수립하게 되고, 중요 정보통신 기반 시설(CIP : Critical Information Infrastructure) 및 회사의 중요 IT 시스템 및 네트웍에 대한 정보 보호를 공동으로 대처하고 전문 조직을 별도로 운영함에 따른 업무 및 비용을 경감할 수 있는 환경을 제공한다.

【대표도】

도 2

【색인어】

ESM, ISAC, CERT, 정보 공유, 분석, 사이버 테러, 해킹, 보안, 침해

【명세서】

【발명의 명칭】

ＩＳＡＣ 형태의 전사적 종합 침해사고 대응시스템 및 방법{ISAC(Information Sharing and Analysis Center System) and CERT(Computer Emergency Response Team) of Information Securit and Management Method Thereof}

【도면의 간단한 설명】

도 1은 종래 개인간 정보 공유 시스템의 구성을 나타낸 구성도,

도 2는 본 발명의 실시예에 따른 전사적 종합 침해사고 대응 시스템의 구성을 나타낸 블럭 구성도,

도 3은 침해 사고 대응 체계를 나타낸 도면,

도 4는 전사적 종합 침해 사고 대응 시스템(ISAC)의 기능별 모델을 나타낸 도면,

도 5는 ISAC의 단계별 체계를 나타낸 블럭 구성도,

도 6은 정보 수집 체계를 나타낸 블럭 구성도,

도 7은 ISAC의 취약점 목록을 수집하는 것을 나타낸 블럭 구성도,

도 8은 스캐너 수집 결과를 나타낸 블럭도,

도 9는 웹 로봇을 이용한 취약점 자동화 수집을 나타낸 블럭도,

도 10은 침해 사고 신고 접수 과정을 나타낸 블럭도,

도 11은 주요 자산에 대한 정보를 수집하는 블럭도,

도 12는 보안 관련 이벤트의 실시간 수집 과정을 나타낸 블럭도,

도 13은 정보 가공/분석 체계를 나타낸 블럭도,

도 14는 데이터웨어 하우징 구축을 나타낸 블럭도,

도 15는 지식 기반 분석 알고리즘이 적용되는 것을 나타낸 블럭도,

도 16은 ISAC의 프로파일 관리기의 구성을 나타낸 블럭도,

도 17은 공유 정보 관리를 나타낸 블럭도,

도 18은 ISAC의 정보 보호 체계를 나타낸 블럭도,

도 19는 타기관/회사 연동 체계를 나타낸 블럭도이다.

< 도면의 주요 부분에 대한 부호의 설명 >

110 : 사용자 컴퓨터

120 : 인터넷

122 : ISP

124 : 라우터

126 : 스위칭 허브

130 : WAP 게이트웨이

140 : WAP 서버

150 : 웹서버

160 : 메일 서버

170 : 정보 공유 서버

180 : 데이터베이스 서버

200 : ISAC

210 : CERT 운영 시스템부

212 : 조기 경보부

214 : 사이버테러 공격평가부

216 : 사고 접수부

218 : 사고접수 데이터베이스

220 : 종합상황 디스플레이부

230 : ESM 관리 시스템부

232 : 컴퓨터 포렌식 데이터베이스

234 : 취약성 데이터베이스

236 : 소스/가공 데이터베이스

238 : 테스트베드

240 : 시스템 점검부

250 : 보안 프로그램부 260 : 보안장치 관리부

270 : 인식장치 관리부

【발명의 상세한 설명】

【발명의 목적】

【발명이 속하는 기술분야 및 그 분야의 종래기술】

<35> 본 발명은 ISAC 형태의 전사적 종합 침해사고 대응시스템 및 방법에 관한 것으로, 더욱 상세하게는 개인이나 민간의 IT 정보, 회사의 정보 등을 원격지에서 상호 간에 공유함과 더불어 해킹이나 사이버 테러 등의 비인가된 접속을 차단하여 침해 사고에 종합적으로 대응할 수 있도록 구성된 ISAC 형태의 전사적 종합 침해사고 대응시스템 및 운영 방법에 관한 것이다.

<36> 인터넷의 확산으로 인해 개인적인 정보가 공유되고 있다. 대표적인 예는 인터넷 사이버 커뮤니티이다. 이러한 커뮤니티는 일반인들 사이에서 동일한 관심이나 취미, 학연, 지연 및 직장 관계 등 서로의 이해 관계가 있는 다수의 인터넷 사용자들이 자신들만의 특정한 인터넷 사이트를 구축하고 그 안에서 상호 간에 정보를 공유하는 것이다.

<37> 기업의 경우, 기업 정보는 기업 운영에 필요한 용도로서 사내적으로 제한적으로 사용하고, 대외적으로는 기업 정보를 공개하는 것은 현실적으로 제한되어 있으며, 강제되지 않는 정보의 공개 즉 기업에서 스스로 선택하여 공개하는 정보의 내용은 대부분 기업의 이미지 향상에 기여할 수 있는 선전성 내용 정도로 제한하고 있다.

<38> 도 1은 종래 개인간 정보 공유 시스템의 구성을 나타낸 구성도이다.

<39> 도 1에 도시된 종래 개인간 정보 공유 시스템은 사용자 컴퓨터(110), 인터넷(120), ISP(122), 라우터(124), 스위칭 허브(126), WAP 서버(140), 웹서버(150), 메일 서버(160), 정보 공유 서버(170), 데이터베이스 서버(180) 등으로 구성된다.

<40> 즉, 하나 이상의 사용자가 사용자 컴퓨터(110)를 통해 인터넷(120)에 물리적으로 접속되어 의기 투합을 위한 정보를 요청하면, 요청된 정보의 제공 경로를 최적화 하는 라우터(124); 정보의 전송 속도를 향상시키기 위하여 수신된 패킷 데이터를 해석하고, 데이터의 최종 목적지를 선별하여 송신하는 스위칭 허브(126); 사용자 컴퓨터(110)의 웹 브라우저에 의해 물리적으로 접속된 상태에서, 하나 이상의 사용자 선택 투합 정보 웹 페이지를 사용자 컴퓨터(110)에 표시하는 웹서버(150); 투합 정보 웹 페이지 상에서 이루어지는 정보 교환을 통해 사용자 상호간에 정보를 공유할 수 있도록 지원하는 정보 공유 서버(170); 사용자 및 사용자의 투합 행위에 해당하는 정보를 저장하는 데이터베이스 서버(180); 사용자 상호간에 맺어진 투합 요청 및 투합 결과 내용을 메일을 통해 자동으로 전송하는 메일 서버(160); 사용자가 이동통신 단말기를 통해 투합 정보를 요청하면 무선 통신망을 통해 전송되는 데이터의 프로토콜을 인터넷(120)에서의 정보 전송 프로토콜로 변환하는 왑(WAP : Wireless Application Protocol, 이하 WAP이라 칭함)게이트웨이(130); WAP 게이트웨이(130)를 통해 전송된 정보 요청 데이터를 수신하여 씨지아이(CGI : Common Gateway Interface)스크립트를 통해 컨텐츠 데이터베이스에 저장된 하나 이상의 컨텐츠 데이터를 검색하여 이동통신 단말기에 표시하는 WAP 서버(140)를 포함한다.

<41> 사용자 컴퓨터(110)는 아이에스피(ISP : Internet Service Provider)(122)를 통해 인터넷(120)에 접속될 수도 있고 랜(LAN)을 통해 접속될 수도 있으며, 웹서버(150)는 하나 이상의 투합 정보 웹 페이지를 사용자 컴퓨터(110)에 제공하는 웹 페이지 호출 모듈을 포함한다.

<42> 정보 공유 서버(170)는 웹 페이지를 통해 사용자의 회원 가입을 처리하는 회원 가입 모듈; 회원 가입된 사용자의 섹션 및 그룹 설정을 지원하는 회원 섹션/그룹 모듈; 사용자의 투합 요청 정보를 수신하여 투합을 원하는 사용자와의 정보 공유를 처리하는 투합 요청 처리 모듈; 하나 이상의 사용자에 대한 투합 요청 내역을 검색하는 투합 검색 모듈; 투합된 사용자 상호간에 홈페이지를 동시에 공유할 수 있도록 지원하는 홈페이지 공유 모듈을 포함한다.

<43> 데이터베이스 서버(180)는 회원으로 가입한 하나 이상의 사용자에 대한 상세 정보를 저장하는 회원 데이터베이스; 회원으로 등록된 사용자의 섹션 및 그룹 설정 내역 정보를 저장하는 섹션/그룹 데이터베이스; 사용자 상호간에 결정된 투합 결과 정보를 저장하는 투합 데이터베이스; 사용자에 의해 선택 가능한 홈페이지 제작 데이터와, 사용자의 선택에 의해 완성된 홈페이지 데이터를 저장하는 홈페이지 데이터베이스를 포함한다.

<44> 상기와 같이 구성된 개인간 정보 공유 시스템은 사용자로 하여금 개인의 관심 분야에 대하여 정보를 분류한 후 섹션별, 그룹별로 개인 정보를 공유할 수 있도록 공유하고자 하는 개인 정보의 섹션 및 그룹을 설정하도록 하고, 하나 이상의 사용자 단말기에 하나 이상의 개인 정보를 표시하여, 개인 정보의 공유을 원하는 사용자와 의기 투합이 이루어지도록 하며, 사용자 상호간에 의기 투합이 이루어지면, 상기 사용자 단말기를 통해 각각의 개인 정보를 공유하여 활용하도록 된 것이다.

<45> 그런데, 상기와 같이 인터넷(120) 상에 정보 공유 서버(170)를 구축해 놓고 다수의 사용자들이 접속하여 정보를 공유할 수 있도록 하고 있으나, 가입되지 않은 미가입자가 악의를 가지고 침입하여 정보를 획득한 후 불의한 일에 사용하는 경우에는 대처하지 못하고 있다. 또한, 악의를 가진 자가 컴퓨터 바이러스 등을 확산시켜 정보를 파괴하는 행위를 포함하여 정보 통신

기반 보호법에 규정된 중요 시설 및 분야에 대한 사이버 테러나 사이버 범죄 등을 일으키고 있다.

<46> 종래에 이러한 해킹 등의 침해 사고를 처리하기 위해서는 피해자가 일일이 해당 시스템에 대한 피해 정도나 관리자, IP, 사고 발생 시점까지의 해당 시스템에 대한 로그/패치 정보, 이력 관리 그리고 백업 등에 관한 것을 전문 기관에 전화로 상담하여 알려주고, 해당 전문 기관에서는 각각의 상담 내용에 대해 수동으로 입력하며, 이를 근거로 침해 사고 내용을 분석하여 판단하는데 그 시간이 며칠에서 몇 주씩 소요되는 불편함이 있다.

<47> 또한, 기업체나 회사에서 전산 담당자들이 이와같은 해킹 등의 공격을 당한 후 문책을 우려하여 컴퓨터에 대해 포맷을 해 버리거나, 로그를 남겨놓지 않은 상태에서 복구하는 데만 관심이 있고, 피해 상황 및 공격자의 정보 등을 발견하여 CERT(Computer Emergency Response Team) 및 사이버 범죄를 담당하는 기관에 신고하여도 범인을 색출하기 힘든 사고가 많이 발생하고 있는 실정이다.

<48> 한편, 개인이나 회사 등의 전산 담당자는 국내외의 CERT 기관 또는 IBM이나 SUN 등의 하드웨어 제작사, 마이크로 소프트 등의 운영 체제 제작사로부터 취약점을 공식 인정된 항목을 일일이 이메일을 통하여 전달받아 대응해야 하는데 매일같이 많은 양이 전달되므로 진위 여부를 판단하기 어려워 패치에 어려움을 겪고 있다. 또한, 상기 기관 등의 홈페이지에 접속하여 현재 운영중인 시스템에 대한 취약성을 점검하여 이를 수동적으로 패치하는 업무를 수행할 수 밖에 없고, 매일 발표되는 새로운 취약점 목록 등의 발표 자료 및 내용이 너무 방대하여, 기관이나 회사에서 1 ~ 2 명의 정보 보호 인력으로는 이를 수용하기에 부담스러워 해킹 등의 요인이 되는 취약성을 방치할 수 밖에 없으며, 이를 통해 실제로 해킹당하는 경우가 허다하였다.

【발명이 이루고자 하는 기술적 과제】

<49> 상기한 문제점을 해결하기 위해 본 발명은, 개인이나 민간의 IT 정보, 회사의 정보 등을 원격지에서 상호 간에 공유함과 더불어 해킹이나 사이버 테러 등의 비인가된 접속을 차단하여 침해 사고에 종합적으로 대응할 수 있도록 구성된 ISAC 형태의 전사적 종합 침해사고 대응시스템 및 방법을 제공함에 목적이 있다.

【발명의 구성 및 작용】

<50> 상기한 목적을 달성하기 위해 본 발명은, 해킹이나 사이버 테러에 의한 사고를 접수하고, 접수한 내용을 분석하여 그에 대한 대처 방안을 제시하는 CERT 운영 시스템부; 큰 기업이나, 은행, 보험 회사를 포함하는 대규모의 기업들의 정보 보호 제품을 통합적으로 관리하는 ESM 관리 시스템부; 상기 사이버 테러를 당한 사고 피해자로부터 사고 내용을 접수하는 사고 접수부; 상기 사이버 테러에 의한 사고에 대해 그 사고 내용을 평가하는 사이버 테러 공격평가부; 상기 사이버 테러에 대해 분석한 내용을 근거로 홈페이지나 이메일로 사이버 테러나 해킹을 사전에 경보하는 기능을 하는 조기 경보부; 접수한 사이버 테러 사고 내용을 데이터로 저장하는 사고접수 데이터베이스; 및 상기 사이버 테러나 해킹의 사고 현황이 디스플레이하는 종합상황 디스플레이부를 포함하는 것을 특징으로 한다.

<51> 또한, 본 발명의 다른 목적에 의하면, 상기와 같이 구성된 시스템의 전사적 종합 침해 사고 대응 방법으로서, (a) 인터넷에서 발견되거나 주요 소스에서 제공되는 각종 취약점과 침해 사고 정보, 다양한 보안 관련 이벤트를 수집하는 정보 수집 단계; (b) 수집된 정보를 가공하고 분석하며 상기 테스트베드를 통해 확인하는 정보 가공/분석 단계; (c) 분석된 정보를 효율적으로 배포, 전파하고, 필요시 위험도별 공격 평가 및 조기 경보 수준을 결정하는 정보 공

유/경보/전파 단계; (d) 구축된 ISAC을 자체 시스템으로 보호하는 정보 보호 단계; (e) 타기관이나 회사와 연동하는 타기관/회사 연동 단계를 포함하는 것을 특징으로 한다.

<52> 이하, 본 발명의 바람직한 실시예를 첨부된 도면들을 참조하여 상세히 설명한다. 우선 각 도면의 구성요소들에 참조부호를 부가함에 있어서, 동일한 구성요소들에 대해서는 비록 다른 도면상에 표시되더라도 가능한 한 동일한 부호를 가지도록 하고 있음에 유의해야 한다. 또한, 본 발명을 설명함에 있어, 관련된 공지 구성 또는 기능에 대한 구체적인 설명이 본 발명의 요지를 흐릴 수 있다고 판단되는 경우에는 그 상세한 설명은 생략한다.

<53> 본 발명은 회사의 중요 정보 시스템 및 전산망 그리고 금융, 통신 등 정보 통신 기반 보호법(법률 6383호) 상에 정의된 주요 정보통신 기반 시설(CIP : Critical Infrastructure Protection) 분야를 보호하는 것을 대상으로하며, 이들 시설 및 시스템에 설치된 방화벽(Firewall), 침입 탐지 시스템(IDS), 바이러스 및 지문을 포함한 생체 인식 제품 등 네트웍 및 물리적인 시스템을 보호하기 위한 다양한 정보 보호 제품 및 시스템을 효율적으로 종합 관리하여 해킹 및 사이버 테러 등 비인가된 접속을 차단, 예방, 복구하는 데에 필요한 기술 및 노하우를 데이터베이스화하고, 이러한 DB 및 정보를 실시간으로 가입 회원 및 타기관/회사의 종업원들과 온라인으로 정보를 공유/분석하고 배포하는 관리 시스템 및 방법에 관한 것이다.

<54> ESM(Enterprise Security Management)은 본래 네트워크나 시스템 리소스들의 각종 위험 요소들을 분석하고 모니터링하는 일종의 "관리 도구"로서 침입 차단 시스템(F/W), 침입 탐지 시스템(IDS), 안티 바이러스 제품 등 기존의 Multi Vendor 보안 솔루션들을 통합 관리함으로서 관리의 효율성을 높이고 능동적인 보안대책을 세울 수 있도록 도와주는 보안 관리 도구로 개발되었다. 하지만, 인터넷 이용의 폭발적인 증가로 이들 정보 보호 시스템에 대한 이벤트 및 로그는 그 정책에 따라 하루 수십메가에서 기가 단위의 많은 데이터를 내놓고 있어서, 관리자들

이 이러한 이벤트에 대한 정확한 대응을 할 수 있는 한계를 초과하여, 요즘은 이를 구별하여 전체적인 이벤트수를 줄이고 진짜 공격을 구별해내서, 위협 요소를 제거하는 연구가 시작되고 있지만 현실적으로 애로사항을 겪고 있으며, 실제 상황에서는 별다른 도움을 못받고 있는 실정이다. 즉, 위험도가 높은 경보나 알람시 이들 시스템에 대하여 수동적으로 과거 보안 및 사고 이력 등을 조사하고, 이미 피해를 입을 상태에서 복구를 해야하는 경우가 비일 비재하기 때문이다.

<55> 최근, 시스템에 저장된 데이터를 보호하기 위한 보안 관리 시스템에 대한 관심이 높아지면서 미국, 유럽 등 선진국들은 이러한 문제를 정부 차원에서 대처하고 있고, 특히 미국은 금융, 통신, 전력, 수송 등의 정보 공유 및 분석 센터(Information Sharing & Analysis Center)를 15 개나 운영하고 있으며, 이를 운영하는 지식 및 노하우를 모두 국가 기밀로 취급해 내용이 공개되어 있지 않다. 우리나라도 정보 통신 기반 보호법 제 16 조에 금융, 통신 등의 정보 공유 및 분석 센터를 설립할 것을 정의하고 있고, 민간 정보 보호 전문 회사들도 이에 대한 대응을 위하여, 침입 차단 시스템이나 침입 감지 시스템, 안티 바이러스 등 종전의 단순한 정보 보호 제품의 이벤트 및 로그 등을 관리하는 ESM(Enterprise Security Management)에서 정보 공유 및 분석(ISAC) 모델을 가미한 종합적인 시스템으로 기술 개발을 추진하고 있다.

<56> 정보 보호 실태에 관한 연구 결과 보고서는 다음과 같은 4가지를 최근 추세로 정리하고 있다.

<57> 1) 조직들이 내.외부로부터 사이버 공격을 받고 있다.

<58> 2) 광범위한 사이버 공격이 탐지되고 있다.

<59> 3) 사이버 공격은 심각한 경제 손실을 초래할 수 있다.

0> 4) 성공적인 공격 방어는 정보 보호 기술 사용 이상의 것을 요구한다.

1> 이러한 실태에 대응하기 위하여 유사한 사이버 테러 및 해킹 위험에 노출될 수 있는 동종 산업별, 또는 동종 기관/회사별로 공동 대응을 위한 침해 사고 대응 및 정보 공유 및 분석 체계(Information Sharing & Analysis Center/System)를 갖추고자, 법령에 의거 각 분야에 대한 센터 설립이 구체화 되고 있지만 이에 적용한 기술 모델이 없어 제각기 추진되고 있는 실정이다.

62> 본 발명은 이미 알려져 있거나 새로 발견된 해킹 및 사이버 테러에 대한 취약점과 대처 방법을 체계적으로 분류하여 사전에 예방할 수 있는 기술적 방법을 제공하며, 광범위하게 탐지되는 위협 요소를 자동적으로 수집, 분류하는 방법을 제공한다.

63> 또한, 본 발명은 해당 조직별로 필요한 정보를 가공하고 분석하는 방법을 제공하고, 효율적으로 공유/전파 및 배포하는 방법을 제공하며, 사이버 테러에 대한 위험도에 따라 조기에 결보하는 방법과 정확한 경보를 할 수 있도록 수준별 사이버 테러 공격을 평가하는 방법을 제공한다.

<64> 그리고, 본 발명은 정보 보호 테스트 베드를 활용한 온라인 교육/훈련 자동화 방법과, 사이버 테러로 인해 공격받은 정보 자산 및 시스템에 대한 자산 평가 및 이에 따른 복구 기간 산정 방법, 컴퓨터 범죄의 증거로 사용할 기초 자료나 데이터베이스 구축 방안을 제공한다.

<65> 도 2는 본 발명의 실시예에 따른 전사적 종합 침해사고 대응 시스템의 구성을 나타낸 블럭 구성도이다.

<66> 본 발명에 따른 전사적 종합 침해사고 대응 시스템(ISAC: 200)은 CERT 운영 시스템부(210), 조기 경보부(212), 사이버테러 공격평가부(214), 사고 접수부(216), 사고접수 데이터베

이스(218), 종합상황 디스플레이부(220), ESM 관리 시스템부(230), 컴퓨터 포렌식 데이터베이스(232), 취약성 데이터베이스(234), 소스/가공 데이터베이스(236), 테스트베드(238), 시스템 점검부(240), 보안 프로그램부(250), 보안장치 관리부(260), 인식장치 관리부(270) 등을 포함한다.

<67> CERT(Computer Emergency Response Team)는 "침해 사고 대응팀"이라고 하며, 해킹 등 외부의 공격을 받은 시스템 관리자가 신고하는 곳을 지칭한다. 국내외 모두 100 여개 기관이 있으며, 최근에는 이러한 소규모로는 대처가 안되서 금융분야 전체, 통신분야 전체 등을 방어하는 ISAC으로 대체되고 있는 중이다.

<68> CERT 운영 시스템부(210)는 해킹이나 사이버 테러에 의한 사고를 접수하고, 접수한 내용을 분석하여 그에 대한 대처 방안을 제시하는 시스템으로서, 각 지점이나 지부에서 접수된 현황을 디스플레이한다.

<69> 조기 경보부(212)는 CERT 운영 시스템부(210)에서 사이버 테러에 대해 분석한 내용을 근거로 홈페이지나 이메일 등으로 사이버 테러나 해킹 등을 사전에 경보하는 기능을 한다. 사이버 테러 공격평가부(214)는 CERT 운영 시스템부(210)가 접수한 사이버 테러 사고에 대해 그 사고 내용을 평가하는 기능을 한다. 사고 접수부(216)는 사이버 테러를 당한 사고 피해자로부터 전화나 팩스, 이메일, 홈페이지 등으로 사고 내용을 접수하는 기능을 한다. 사고접수 데이터베이스(218)는 CERT 운영 시스템부(210)가 접수한 사고 내용을 데이터로 저장하며, 종합상황 디스플레이부(220)는 각 지점이나 각 지부, 각 기관으로부터의 사이버 테러나 해킹 등의 사고 현황이 디스플레이된다.

<70> ESM 관리 시스템부(230)는 기업 통합 정보보호 관리시스템으로서, 큰 기업, 은행, 보험, 통신 사업자 등 대규모의 기업들이 정보 보호 제품(Firewall, IDS 등)을 통합적으로 관리하는

시스템이다. 이는 주요 정보 보호 제품들을 한 곳으로 묶어주는 콘솔과 같은 역할을 하며, 정확한 정보들을 집산하여 정리하는 기능을 한다.

<71> 컴퓨터 포렌식 데이터베이스(232)는 사이버 테러나 해킹에 대해 수사하고 법정에 제소할 수 있는, 즉 법적 증거 기능을 할 수 있는 자료를 모아 놓은 데이터베이스이다. 이는 해커가 특정 회사의 중요 시스템을 마비시키거나 파일 전체를 삭제하면 그 회사는 중대한 경영 위기와 경제적인 손실을 입게 되므로 이를 방지하거나 보상받기 위해 법적인 증거 자료가 필요한 것이다.

<72> 취약성 데이터베이스(234)는 해커가 모든 컴퓨터나 데이터베이스, 운영 체제(OS), 네트워크 장비의 소프트웨어로 외부에서 접속할 수 있는 취약 부분을 데이터로 저장하고 있다.

<73> 소스/가공 데이터베이스(236)는 소프트웨어에 대한 소스 및 가공된 소프트웨어 소스를 저장하고 있으며, 테스트베드(238)는 원격지에서 사용자가 시뮬레이션을 통해 해커나 사이버 테러 등을 실행해 볼 수 있도록 제공하는 프로그램이다.

<74> 시스템 점검부(240)는 네트워크 스캐너나, 시스템 스캐너, 분배 스캐너, 바이러스 스캐너 등을 점검하기 위한 시스템이고, 보안 프로그램부(250)는 방화벽이나 IDS, 바이러스 백신, 보안 운영 체제 등의 보안 관련 프로그램을 관리한다.

<75> 보안장치 관리부(260)는 침입 차단 시스템이나, VPN 시스템, 침입 탐지 시스템, 해킹 역추적 시스템, EAM 시스템, 자원 관리 시스템, 워커마킹 시스템 등의 장치를 관리하며, 인식장치 관리부(270)는 카드문 인식이나, RF 카드 인식, 장평 인식, 홍채 인식, 지문 인식, 무게 감지 인식 등의 인식 장치들을 관리한다.

<76> 도 3은 사이버 테러 침해 사고가 발생했을 때의 처리 흐름도를 나타낸 것으로서 침해 사고 대응 체계를 나타낸 것이다.

<77> 도 3에 도시된 바와 같이 사이버 테러 침해 사고 발생시 보안 관제 시스템(ESM)이 관리하는 보안 장치 관리부(260)의 침입 탐지 시스템에서 알람을 발생시키고, 전사적 종합 침해사고 대응 시스템(200)은 사고 접수부(216)를 통해 침해 사고를 접수한다. 이때, 침해 사고 접수는 웹 페이지나, 전화, 팩스, 이메일로도 접수한다.

<78> CERT 운영 시스템부(210)는 침해 사고 접수 정보를 사고 접수 데이터베이스(218)에 저장한 후, 이를 근거로 보안 관제 로그와 보안 이력을 바탕으로 취약점을 분석한다. 이때, 사이버 테러 공격평가부(214)에서 공격 내용에 대해 평가한다. 그리고 사고 내용에 대해 분석한 것을 근거로 다음 테러 사고에 대비해 사전에 경고할 내용에 대해 조기 경보부(212)를 통해 홈페이지나 이메일로 조기 경보함으로써 사이버 테러 사고에 대해 대응 처리한다.

<79> 보안 관제 시스템인 ESM 관리 시스템부(230)가 침해 사고 결과를 CERT 운영 시스템부(210)에 보고함으로써 취약성 데이터베이스(234)에 저장하게 된다.

<80> 도 4는 전사적 종합 침해사고 대응 시스템(200)의 기능별 모델을 나타낸 것이다.

<81> ISAC(200)은 지원 센터, 사고 접수 지원, 경보/모니터링, 연구 개발, 테스트베드, 취약성 DB, 도구 DB 등으로 구성되고, 테스트베드는 계획, 정책/지침, 교육/훈련 등으로 나뉜다. 취약성 DB에는 일반 정보, V.DB(취약성 DB), Patch DB, 기초 DB, Attack DB(공격용 기법 DB) 등으로 구성되고, 도구 DB는 Advisory DB, Defense DB(방어용 기법 DB) 등으로 구성된다.

<82> 도 5는 ISAC(200)의 단계별 체계를 나타낸 블럭 구성도이다.

<83> ISAC(200)은 정보 수집 체계, 정보 가공/분석 체계, 정보 공유/경보/전파 체계, ISAC 센터 정보 보호 체계, 타기관/회사 연동 체계 등으로 구성된다.

<84> 정보 수집 체계는 각종 취약점고 침해 사고 정보, 다양한 보안 관련 이벤트를 수집하고, 정보 가공/분석 체계는 수집된 정보를 가공하고 분석하며, 테스트베드를 통하여 확인한다.

<85> 정보 공유/경보/전파 체계는 분석된 정보를 효율적으로 배포, 전파하고, 필요시 위험도별 공격 평가 및 조기 경보 수준을 결정한다. ISAC 센터 정보 보호 체계는 구축된 정보 공유/분석 시스템을 자체 시스템으로 보호하기 위한 장치이다. 타기관/회사 연동 체계는 타 기관/CERT/ISAC 등과 정보 공유/분석 시스템과의 연계를 위한 방법이다.

<86> 도 6은 도 5의 정보 수집 체계를 나타낸 블럭 구성도이다.

<87> 정보 수집 체계는 인터넷 등에서 발견되거나 주요 소스에서 제공 되어지는 취약점 목록을 수집하는 부분과, 주기적으로 점검하고 발견된 취약점 결과를 수집하는 부분, 각종 해킹 도구나 대처 방법 등의 보안 자료를 수집하는 부분, 최신의 컴퓨터 바이러스 정보를 수집하는 부분, 침해 사고로 판단되는 신고를 통하여 침해사고 수집 부분, 보호하여야 하는 주요 시스템 자산의 정보를 수집하는 부분, 정보공유 및 분석 센터(ISAC) 구현 방법을 통하여 각종 보안 제품들로부터 발생되는 이벤트를 수집하는 부분 등으로 구성되며 수집된 정보는 정형화된 형태의 가공된 데이터베이스로 저장된다.

<88> 도 7은 도 5의 ISAC의 취약점 목록을 수집하는 것을 나타낸 블럭 구성도이다.

<89> 취약점 목록을 수집하는 부분은 국내 외의 여러 기관 또는 시스템 하드웨어 제작사, 운영체제 제작사로부터 취약점으로 공식 인정된 항목을 DB 관리기를 통하여 분류 가공하여 입력하는 것을 말한다.

<90> 하드웨어 제작사로부터 일반 정보나 패치 정보를 입력받고, 운영 체제 제작사로부터 버전 정보, 패치 정보, 취약점(문제점), 대책 등을 입력받으며, 어플리케이션 제작사로부터 버전 정보, 패치 정보, 취약점/대책을 입력받고, 국내외 정보 수집 기관으로부터 Common Vulnerabilities and Exposures (CVE) 등 취약점 DB를 제공받는다.

<91> 도 8은 스캐너 수집 결과를 나타낸 블럭도이다.

<92> 취약점을 주기적으로 점검하고 발견된 취약점 결과를 수집하는 부분은 취약점 분석을 위한 네트워크 기반의 스캐너와 시스템 호스트 기반의 스캐너를 이용하여 사용관리자가 설정된 시간에 주기적으로 점검하거나 필요시 수시로 점검된 결과를 수집하는 과정이다.

<93> 도 9는 웹 로봇을 이용한 취약점 자동화 수집을 나타낸 블럭도이다.

<94> 각종해킹도구나 보안관련 자료, 최신의 컴퓨터 바이러스 정보 등을수집하는 부분은 웹(Web) 로봇(Robot)과 같은 자동화된 수집도구를 사용하거나 참고문헌 등을 통해 주기적으로 수집하는 과정이다.

<95> 도 10은 침해 사고 신고 접수 과정을 나타낸 블럭도이다.

<96> 침해 사고 신고 부분은 정보 공유 시스템에 참여하는 기관의 구성원들로부터 해킹 또는 바이러스에 의한 침해 사고를 전화, FAX, Mail 등의 통신 수단과 Web을 통해 직접 신고할 수 있는 모든 수단을 포함하여 신고를 접수하는 과정이다.

<97> 도 11은 주요 자산에 대한 정보를 수집하는 블럭도이다.

<98> 보호하고자 하는 주요 자산에 대한 정보를 수집하는 부분은 참여 기관의 주요 시스템, 네트워크 다바이스 등의 정보와 그 자산의 중요도(자산가치) 등을 정형화하여 수집하는 과정이다.

<99> 도 12는 보안 관련 이벤트의 실시간 수집 과정을 나타낸 블럭도이다.

100> 보안과 관련된 주요 이벤트를 수집하는 부분은 통합 관리 대상인 침입 차단 시스템, 침입 탐지 시스템, 정책 관리 시스템, 컴퓨터 방역 시스템, PC 보안 시스템, 역추적시스템, 인증 시스템, 네트워크 장비 등의 이벤트를 실시간으로 수집하는 과정이다.

101> 도 13은 정보 가공/분석 체계를 나타낸 블럭도이다.

102> 정보 가공/분석 체계는 수집된 대용량의 정보를 효율적으로 구축하기 위한 데이터웨어 하우징 부분과 데이터 마이닝 또는 지식 기반의 분석 알고리즘이 적용되는 분석 부분으로 구성된다.

103> 도 14는 데이터웨어 하우징 구축을 나타낸 블럭도이다.

104> 대용량의 수집된 정보를 데이터웨어 하우징으로 구축하는 부분은 정보 수집 체계의 각종 수집되는 자료의 형태를 여러가지 분류로 검색 및 가공이 가능하도록 정규화하여 데이터베이스로 구축하는 과정이다.

105> 즉, 데이터를 입력하고 데이터 유형별로 분류한 후, 요약/가공 여부를 판단해 검색 유형별로 요약한다거나, 데이터 필드를 추가하여 데이터베이스를 생성하는 것이다.

106> 도 15는 지식 기반 분석 알고리즘이 적용되는 것을 나타낸 블럭도이다.

107> 지식 기반의 분석 알고리즘이 적용되는 부분은 도 13과 같이 구축된 데이터베이스로부터 각종 침해 사고 및 취약점, 그리고 도 10에서 수집된 주요 자산 정보들과의 상관 관계, 인식 가능한 패턴, 이를 예방하는 위한 분류 방법 등 각종 분석을 위한 알고리즘을 관리(알고리즘 DB에 추가, 변경, 삭제 포함)하고 분석을 수행하는 과정이다.

108> 도 16은 ISAC의 프로파일 관리기의 구성을 나타낸 블럭도이다.

109> 공유되는 정보의 유형 분류, 사용자/기관별 공유 범위를 관리하는 부분과 웹(Web)을 포함하는 가장 일반적인 정보 공유 수단을 이용하여 정보 수집 체계에서 수집된 공유 가능한 정보를 검색 등의 기능을 제공하는 부분, 분류 및 가공된 정보를 이메일, 전화, FAX, 문자 메세지 등 표현 가능한 매체를 통하여 신속하게 전파하는 부분으로 구성된다.

110> 도 17은 공유 정보 관리를 나타낸 블럭도이다.

111> 공유하고자 하는 정보를 관리하는 부분은 정보를 이용하는 사용자의 등급을 등급 체계에 따라 관리하고, 공유될 정보도 분류 유형과 내용에 따라 모든 참여 기관에 제공될 정보와 참여 기관별로 별도로 제공될 정보 등의 범위에 대한 관리가 이루어지는 과정이다.

112> 각종 이용 가능한 전송 수단과 매체를 이용하여 정보를 제공하는 부분은 도 15에서 분류된 등급과 정보의 내용을 유/무선 전송 매체(전화, FAX, Mail, 문자 메세지 등)와 웹(Web)을 이용하여 필요한 정보를 검색하고 검색된 정보를 제공하는 과정이다. 제공되는 정보의 내용 중 긴급 사항 또는 모든(또는 특정) 사용자에게 전파하는 부분은 도 17의 과정과 유사하나 상기 부분과의 차이는 도 17의 경우 사용자의 요청에 의해서 이루어지나 여기서는 사용자의 요청과 무관하게 정보의 내용이 전파된다는 것이다.

113> 도 18은 ISAC의 정보 보호 체계를 나타낸 블럭도이다.

114> 구축된 정보 공유/분석 시스템 자체 보호를 위하여 설치된 장소의 물리적 보안 (카드 인증, 비밀번호키, 생체인식 등 구현 가능한 모든 수단 포함) 부분과 자체 시스템 보호를 위한 보안 시스템(공인인증서 기반의 인증시스템 , 침입차단, 침입탐지, 바이러스차단, 자원관리, 워터마킹 암호화, 문서보안, 역추적 등 구현 가능한 네트워크 및 시스템 보호 수단 포함) 부분으로 구성된다.

:115> 도 19는 타기관/회사 연동 체계를 나타낸 블럭도이다.

:116> 타 기관/CERT 등과 정보 공유/분석 시스템과의 연계를 위한 방법은 요약되고 상호 교환될 정보를 연동하기 위한 기능을 제공하기 위한 기관 정보를 관리하는 부분과 실제로 인터페이스를 담당하는 부분으로 구성된다.

:117> 즉, 상기와 같이 구성된 전사적 종합 침해사고 대응시스템은 다음과 같은 과정으로 침해사고에 대응하게 된다.

:118> 1) 정보 수집 단계

:119> 2) 정보 가공/분석 단계

:120> 3) 정보 공유/경보/전파 단계

:121> 4) 정보 보호 단계

:122> 5) 타기관/회사 연동 단계

:123> 상기 정보 수집 단계에 있어서, 침해 사고 정보는 팩시밀리나, 웹 페이지, 이메일 등으로 수집하거나, 통합 보안 관리 등으로 자동화하여 수집할 수 있다. 또한 수집된 정보는 분류하게 된다.

:124> 그리고, 수집하는 보안 이벤트 중에서 침해 사고 또는 침해를 야기할 수 있는 정보를 추출하며, 이에 대해 자동으로 침해 사고를 접수한다.

125> 사이버 테러에 대한 위험도에 따른 조기 경보를 실행하며, 정확한 경보를 할 수 있도록 사이버 테러 공격을 평가하여 수준별로 나누게 된다.

126> 정보 보호 테스트베드를 통해 원격지에서 사용자가 온라인으로 사이버 테러 교육/훈련 등을 실행할 수 있으며, 시뮬레이션을 통해 간접적으로 경험할 수도 있다.

127> 사이버 테러로 인해 공격받은 정보 자산 및 시스템에 대한 자산 평가를 수행하고, 이에 따른 복구 기간을 산정할 수 있으며, 사고시 컴퓨터 범죄의 증거로 사용할 기초 자료를 데이터베이스화하여 보관한다.

128> 이상의 설명은 본 발명의 기술 사상을 예시적으로 설명한 것에 불과한 것으로서, 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자라면 본 발명의 본질적인 특성에서 벗어나지 않는 범위에서 다양한 수정 및 변형이 가능할 것이다. 따라서, 본 발명에 개시된 실시예들은 본 발명의 기술 사상을 한정하기 위한 것이 아니라 설명하기 위한 것이고, 이러한 실시예에 의하여 본 발명의 기술 사상의 범위가 한정되는 것은 아니다. 본 발명의 보호 범위는 아래의 청구범위에 의하여 해석되어야 하며, 그와 동등한 범위 내에 있는 모든 기술 사상은 본 발명의 권리범위에 포함되는 것으로 해석되어야 할 것이다.

【발명의 효과】

129> 이상에서 설명한 바와 같이 본 발명에 의하면, 자동화되고 체계적인 해킹/사이버테러 등 침해 사고 대응 체계를 수립하게 되고, 정보통신 기반 시설 및 회사의 중요 IT 시스템 및 네트웍에 대한 정보 보호를 공동으로 대처하고 전문 조직을 별도로 운영함에 따른 업무 및 비용을 경감하여, 정보 수집 및 적용, 기술 확보, 인력 및 조직 운영 등 모든 요소들에 대한 문제를 경감할 수 있는 환경을 제공한다.

【특허청구범위】

【청구항 1】

해킹이나 사이버 테러에 의한 사고를 접수하고, 접수한 내용을 분석하여 그에 대한 대처 방안을 제시하는 CERT 운영 시스템부(210);

큰 기업이나, 은행, 보험 회사를 포함하는 대규모의 기업들의 정보 보호 제품을 통합적으로 관리하는 ESM 관리 시스템부(230);

상기 사이버 테러를 당한 사고 피해자로부터 사고 내용을 접수하는 사고 접수부(216);

상기 사이버 테러에 의한 사고에 대해 그 사고 내용을 평가하는 사이버 테러 공격평가부(214);

상기 사이버 테러에 대해 분석한 내용을 근거로 홈페이지나 이메일로 사이버 테러나 해킹을 사전에 경보하는 기능을 하는 조기 경보부(212);

접수한 사이버 테러 사고 내용을 데이터로 저장하는 사고접수 데이터베이스(218); 및

상기 사이버 테러나 해킹의 사고 현황이 디스플레이하는 종합상황 디스플레이부(220)

를 포함하는 것을 특징으로 하는 전사적 종합 침해 사고 대응 시스템.

【청구항 2】

제 1 항에 있어서,

상기 사이버 테러나 해킹에 대해 수사하고 법정에 제소할 수 있는 법적 증거 자료를 모아 놓은 컴퓨터 포렌식 데이터베이스(232);

해커가 모든 컴퓨터나 데이터베이스, 운영 체제(OS), 네트워크 장비의 소프트웨어로 외부에서 접속할 수 있는 취약 부분을 데이터로 저장하고 있는 취약성 데이터베이스(234);

소프트웨어에 대한 소스 및 가공된 소프트웨어 소스를 저장하고 있는 소스/가공 데이터베이스(236);

사용자가 원격지에서 해킹이나 사이버 테러를 실행해 볼 수 있도록 시뮬레이션 프로그램을 제공하는 테스트베드(238);

다수의 스캐너 장치를 점검하기 위한 시스템 점검부(240);

방화벽이나 IDS, 바이러스 백신, 보안 운영 체제를 포함하는 보안 관련 프로그램을 관리하는 보안 프로그램부(250);

다수의 보안 장치를 관리하는 보안장치 관리부(260); 및

다수의 인식 장치들을 관리하는 인식장치 관리부(270)

를 추가로 더 포함하는 것을 특징으로 하는 전사적 종합 침해 사고 대응 시스템.

【청구항 3】

CERT 운영 시스템부(210), 조기 경보부(212), 사이버테러 공격평가부(214), 사고접수부(216), 사고접수 데이터베이스(218), 종합상황 디스플레이부(220), ESM 관리 시스템부(230), 컴퓨터 포렌식 데이터베이스(232), 취약성 데이터베이스(234), 소스/가공 데이터베이스(236), 테스트베드(238), 시스템 점검부(240), 보안 프로그램부(250), 보안장치 관리부(260), 인식장치 관리부(270)를 구비하는 시스템의 전사적 종합 침해 사고 대응 방법으로서,

(a) 인터넷에서 발견되거나 주요 소스에서 제공되는 각종 취약점과 침해 사고 정보, 다양한 보안 관련 이벤트를 수집하는 정보 수집 단계;

(b) 수집된 정보를 가공하고 분석하며 상기 테스트베드를 통해 확인하는 정보 가공/분석 단계;

(c) 분석된 정보를 효율적으로 배포, 전파하고, 필요시 위험도별 공격 평가 및 조기 경보 수준을 결정하는 정보 공유/경보/전파 단계;

(d) 구축된 ISAC을 자체 시스템으로 보호하는 정보 보호 단계;

(e) 타기관이나 회사와 연동하는 타기관/회사 연동 단계

를 포함하는 것을 특징으로 하는 전사적 종합 침해 사고 대응 방법.

【청구항 4】

제 3 항에 있어서, 상기 단계 (a)는,

인터넷에서 발견되거나 주요 소스에서 제공되어지는 취약점 목록을 수집하는 부분과, 주기적으로 점검하고 발견된 취약점 결과를 수집하는 부분, 각종 해킹 도구나 대처 방법의 보안 자료를 수집하는 부분, 최신의 컴퓨터 바이러스 정보를 수집하는 부분, 침해 사고로 판단되는 신고를 통하여 침해 사고 수집 부분, 보호하여야 하는 주요 시스템 자산의 정보를 수집하는 부분, ISAC을 통하여 각종 보안 제품들로부터 발생되는 이벤트를 수집하는 부분을 포함하는 것을 특징으로 하는 전사적 종합 침해 사고 대응 방법.

【청구항 5】

제 4 항에 있어서,

상기 취약점 목록을 수집하는 부분은 국내 외의 여러 기관 또는 시스템 하드웨어 제작사, 운영체제 제작사로부터 취약점으로 공식 인정된 항목을 DB 관리기를 통하여 분류 가공하여 입력하는 것을 특징으로 하는 전사적 종합 침해 사고 대응 방법.

【청구항 6】

제 4 항에 있어서,

상기 취약점 결과를 수집하는 부분은 취약점 분석을 위한 네트워크 기반의 스캐너와 시스템 호스트 기반의 스캐너를 이용하여 사용관리자가 설정된 시간에 주기적으로 점검하거나 필요시 수시로 점검된 결과를 수집하는 것을 특징으로 하는 전사적 종합 침해 사고 대응 방법.

【청구항 7】

제 4 항에 있어서,

각종 해킹 도구나 대처 방법의 보안 자료를 수집하는 부분은 웹(Web) 로봇(Robot)과 같은 자동화된 수집 도구를 사용하거나 참고 문헌을 통해 주기적으로 수집하는 것을 특징으로 하는 전사적 종합 침해 사고 대응 방법.

【청구항 8】

제 4 항에 있어서,

상기 침해 사고 수집 부분은 ISAC에 참여하는 기관의 구성원들로부터 해킹 또는 바이러스에 의한 침해 사고를 전화, 팩시밀리, 이메일을 포함하는 통신 수단과 웹을 통해 직접 신고할 수 있는 모든 수단을 포함하여 신고를 접수하는 것을 특징으로 하는 전사적 종합 침해 사고 대응 방법.

【청구항 9】

제 4 항에 있어서,

상기 주요 시스템 자산의 정보를 수집하는 부분은 참여 기관의 주요 시스템, 네트워크 다바이스의 정보와 그 자산의 중요도(자산가치)를 정형화하여 수집하는 것을 특징으로 하는 전사적 종합 침해 사고 대응 방법.

【청구항 10】

제 4 항에 있어서,

상기 주요 이벤트를 수집하는 부분은 통합 관리 대상인 침입 차단 시스템, 침입 탐지 시스템, 정책 관리 시스템, 컴퓨터 방역 시스템, PC 보안 시스템, 역추적 시스템, 인증 시스템, 네트워크 장비의 이벤트를 실시간으로 수집하는 것을 특징으로 하는 전사적 종합 침해 사고 대응 방법.

【청구항 11】

제 3 항에 있어서, 상기 단계 (b)는,

수집된 대용량의 정보를 효율적으로 구축하기 위한 데이터웨어 하우징 부분과 데이터 마이닝 또는 지식 기반의 분석 알고리즘이 적용되는 분석 부분으로 구성된 것을 특징으로 하는 전사적 종합 침해 사고 대응 방법.

【청구항 12】

제 11 항에 있어서,

상기 데이터웨어 하우징 부분은 각종 수집되는 자료의 형태를 여러가지 분류로 검색 및 가공이 가능하도록 정규화하여 데이터베이스로 구축하는 것을 특징으로 하는 전사적 종합 침해 사고 대응 방법.

【청구항 13】

제 11 항에 있어서,

상기 지식 기반의 분석 알고리즘이 적용되는 부분은 구축된 데이터베이스로부터 각종 침해 사고 및 취약점, 그리고 수집된 주요 자산 정보들과의 상관 관계, 인식 가능한 패턴, 이를 예방하기 위한 분류 방법이 포함된 각종 분석을 위한 알고리즘을 관하고 분석을 수행하는 것을 특징으로 하는 전사적 종합 침해 사고 대응 방법.

【청구항 14】

제 3 항에 있어서, 상기 단계 (c)는,

공유되는 정보의 유형 분류, 사용자/기관별 공유 범위를 관리하는 부분과 웹(Web)을 포함하는 가장 일반적인 정보 공유 수단을 이용하여 정보 수집 체계에서 수집된 공유 가능한 정보를 검색의 기능을 제공하는 부분, 분류 및 가공된 정보를 이메일, 전화, FAX, 문자 메세지를 포함한 표현 가능한 매체를 통하여 신속하게 전파하는 부분으로 구성된 것을 특징으로 하는 전사적 종합 침해 사고 대응 방법.

【청구항 15】

제 14 항에 있어서,

상기 공유하고자 하는 정보를 관리하는 부분은, 정보를 이용하는 사용자의 등급을 등급 체계에 따라 관리하고, 공유될 정보도 분류 유형과 내용에 따라 모든 참여 기관에 제공될 정보와 참여 기관별로 별도로 제공될 정보의 범위에 대한 관리가 이루어지는 것을 특징으로 하는 전사적 종합 침해 사고 대응 방법.

【청구항 16】

제 14 항에 있어서,

상기 각종 이용 가능한 전송 수단과 매체를 이용하여 정보를 제공하는 부분은, 분류된 등급과 정보의 내용을 유/무선 전송 매체와 웹을 이용하여 필요한 정보를 검색하고 검색된 정보를 제공하는 것을 특징으로 하는 전사적 종합 침해 사고 대응 방법.

【청구항 17】

제 3 항에 있어서, 상기 단계 (d)는,

구축된 ISAC 시스템 자체 보호를 위하여 설치된 장소의 물리적 보안 부분과 자체 시스템 보호를 위한 보안 시스템 부분으로 구성된 것을 특징으로 하는 전사적 종합 침해 사고 대응 방법.

【청구항 18】

제 3 항에 있어서, 상기 단계 (e)는,

요약되고 상호 교환될 정보를 연동하기 위한 기능을 제공하기 위한 기관 정보를 관리하는 부분과 실제로 인터페이스를 담당하는 부분으로 구성된 것을 특징으로 하는 전사적 종합 침해 사고 대응 방법.

【청구항 19】

제 3 항에 있어서,

상기 단계 (b)의 테스트베드는 사용자가 원격지에서 해킹이나 사이버 테러를 실행해 볼 수 있도록 시뮬레이션 프로그램을 제공하는 것을 특징으로 하는 전사적 종합 침해 사고 대응 방법.

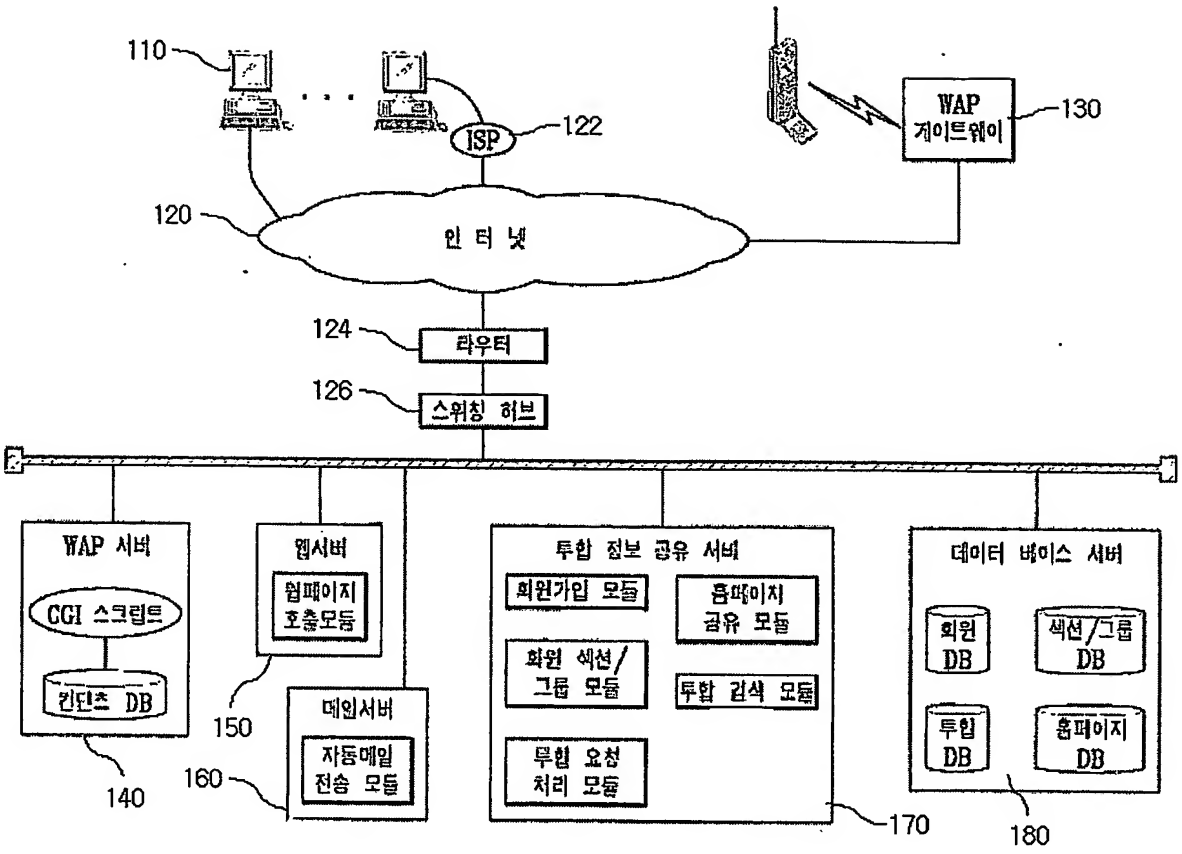
【청구항 20】

제 3 항에 있어서,

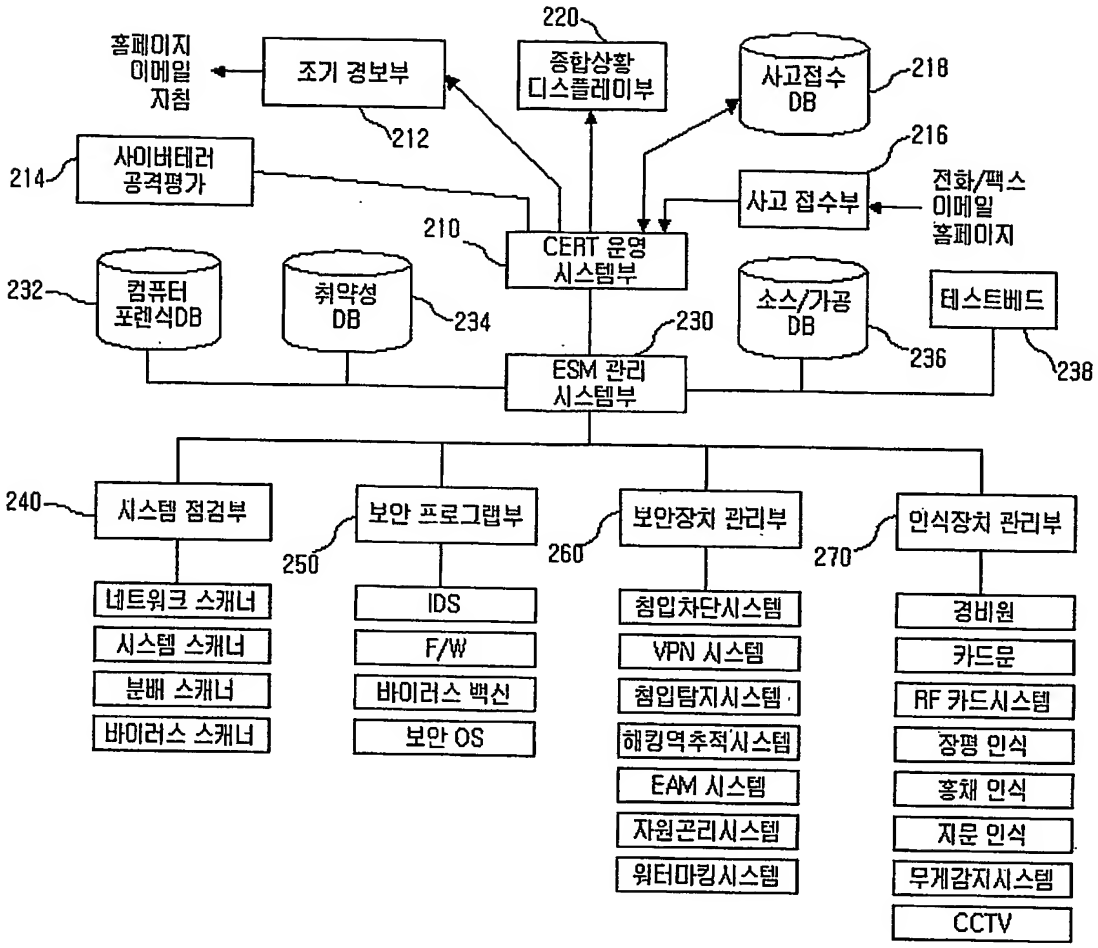
상기 ISAC은 상기 사이버 테러나 해킹에 대해 수사하고 법정에 제소할 수 있는 법적 증거 자료를 상기 컴퓨터 포렌식 데이터베이스(232)에 모아 놓은 것을 특징으로 하는 전사적 종합 침해 사고 대응 방법.

【도면】

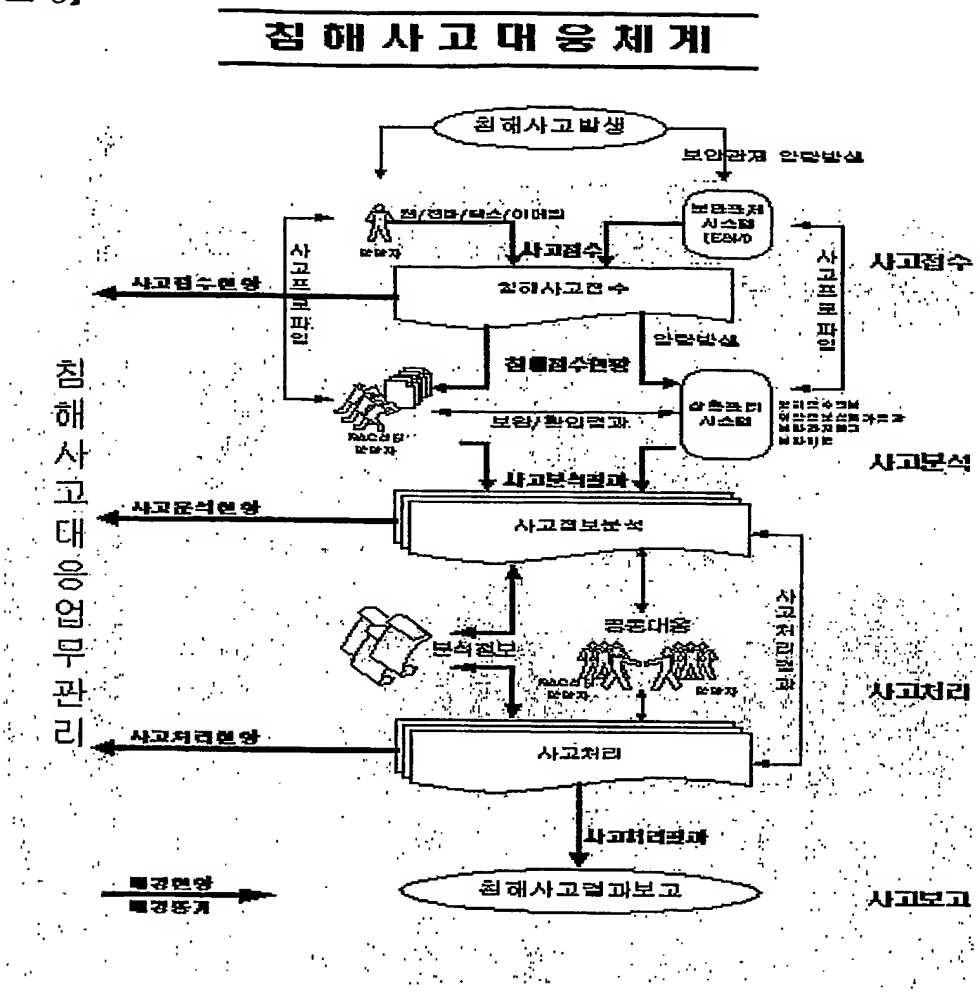
【도 1】


110
ISP
122
WAP
게이트웨이
130
120
인 터 넷
124
라우터
126
스위칭 허브
WAP 서버
CGI 스크립트
컨텐츠 DB
140
웹서버
웹페이지
호출모듈
150
메일서버
자동메일
전송 모듈
160
투합 정보 공유 서버
회원가입 모듈
홈페이지
공유 모듈
회원 섹션/
그룹 모듈
투합 검색 모듈
무합 요청
처리 모듈
170
데이터 베이스 서버
회원
DB
섹션/그룹
DB
투합
DB
홈페이지
DB
180

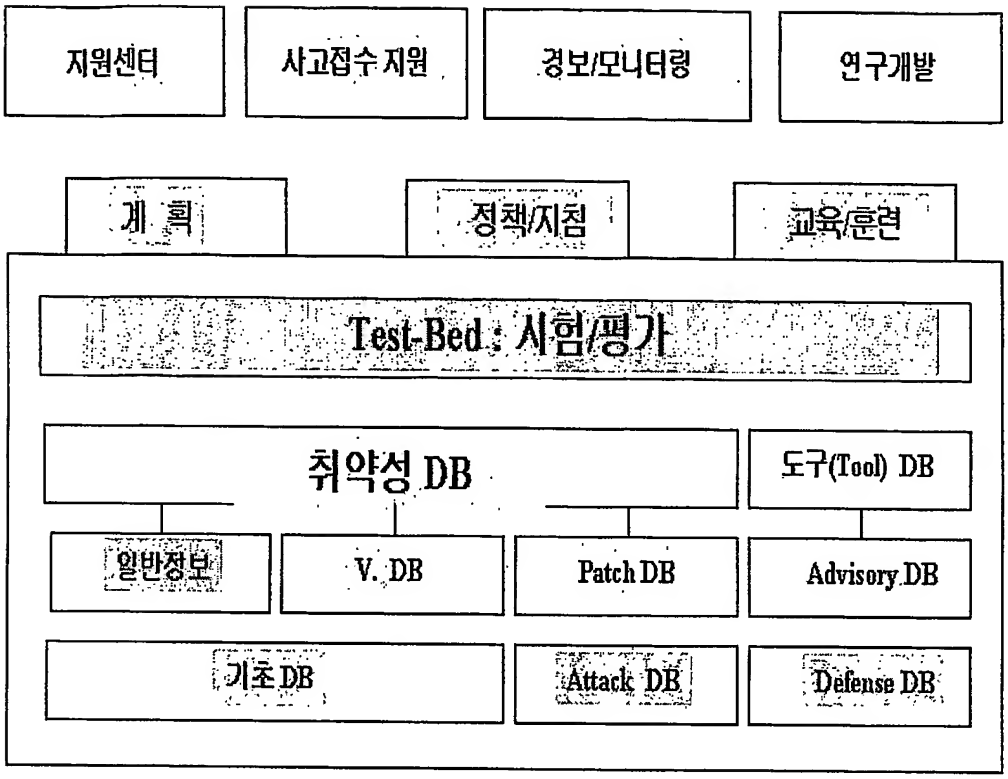
【도 2】


220
홈페이지
이메일
지침
조기 경보부
종합상황
디스플레이부
사고접수
DB
218
212
216
214
사이버테러
공격평가
사고 접수부
전화/팩스
이메일
홈페이지
210
CERT 운영
시스템부
232
컴퓨터
포렌식DB
취약성
DB
234
230
소스/가공
DB
테스트베드
236
238
ESM 관리
시스템부
240
시스템 점검부
250
보안 프로그램부
260
보안장치 관리부
270
인식장치 관리부
네트워크 스캐너
시스템 스캐너
분배 스캐너
바이러스 스캐너
IDS
F/W
바이러스 백신
보안 OS
침입차단시스템
VPN 시스템
침입탐지시스템
해킹역추적시스템
EAM 시스템
자원관리시스템
워터마킹시스템
경비원
카드문
RF 카드시스템
장평 인식
홍채 인식
지문 인식
무게감지시스템
CCTV

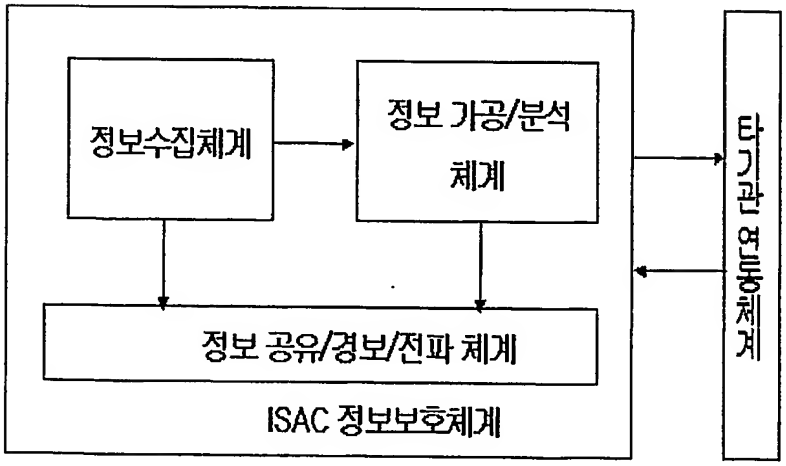
【도 3】


침 해 사 고 대 응 체 계
침해사고대응업무관리
침해사고발생
보안관제 알람발생
보안프로그램 시스템 (ESM)
전/전화/팩스/이메일
사고접수
사고프로파일
사고접수현황
침해사고접수
알람발생
침해접수현황
보완/확인결과
사고분석결과
사고분석현황
사고정보분석
분석정보
공동대응
사고처리결과
사고처리현황
사고처리
사고처리결과
침해사고결과보고
특경현황
특경통계
사고접수
사고분석
사고처리
사고보고

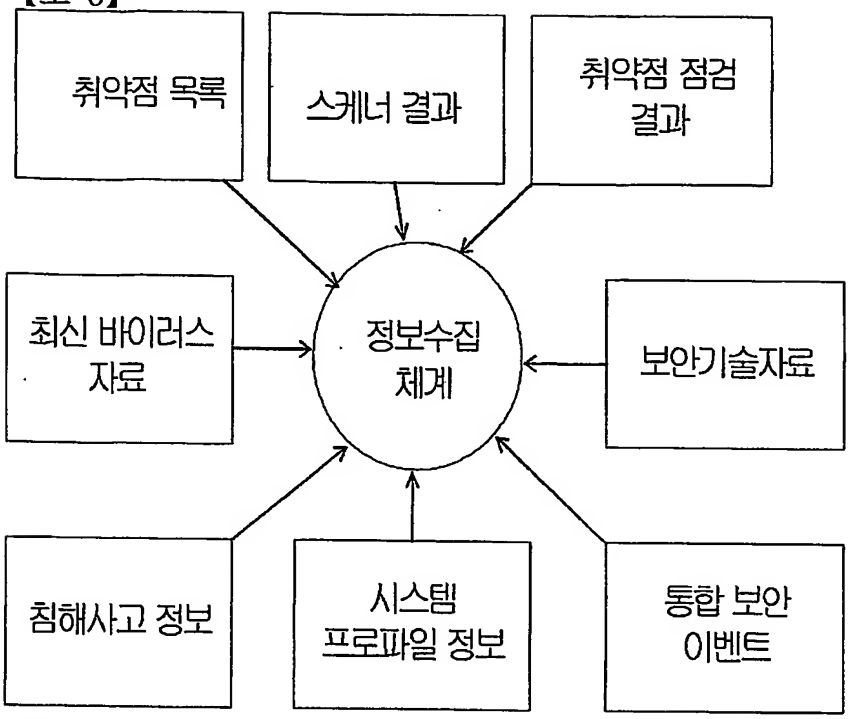
【도 4】


지원센터
사고접수 지원
경보/모니터링
연구개발
계 획
정책/지침
교육/훈련
Test-Bed : 시험/평가
취약성 DB
도구(Tool) DB
일반정보
V. DB
Patch DB
Advisory DB
기초 DB
Attack DB
Defense DB

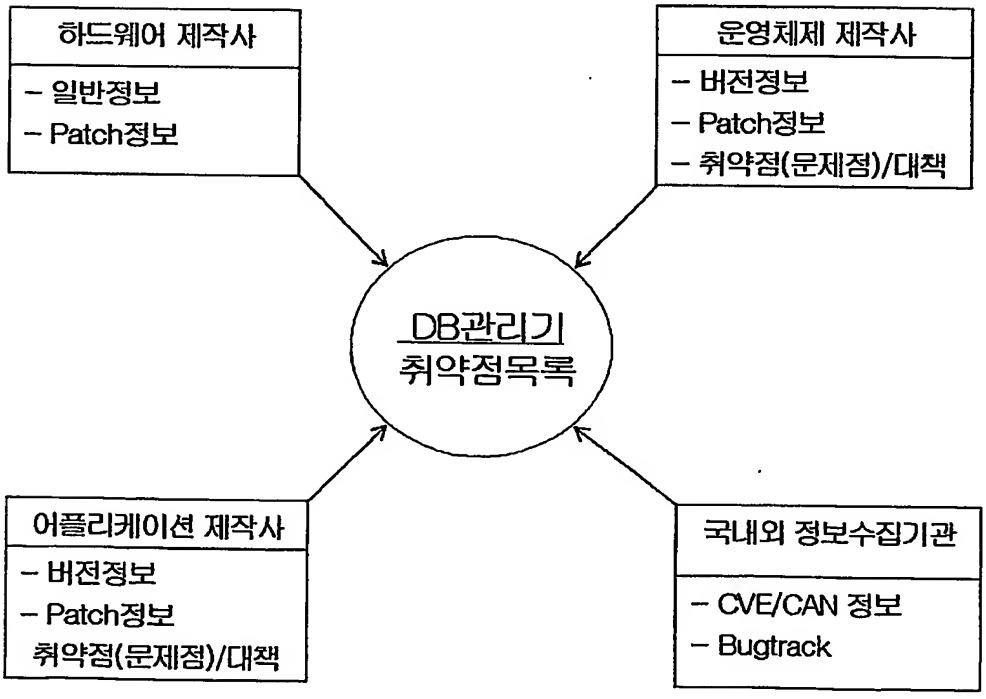
【도 5】


정보수집체계
정보 가공/분석 체계
정보 공유/경보/전파 체계
ISAC 정보보호체계
타기관 연동체계

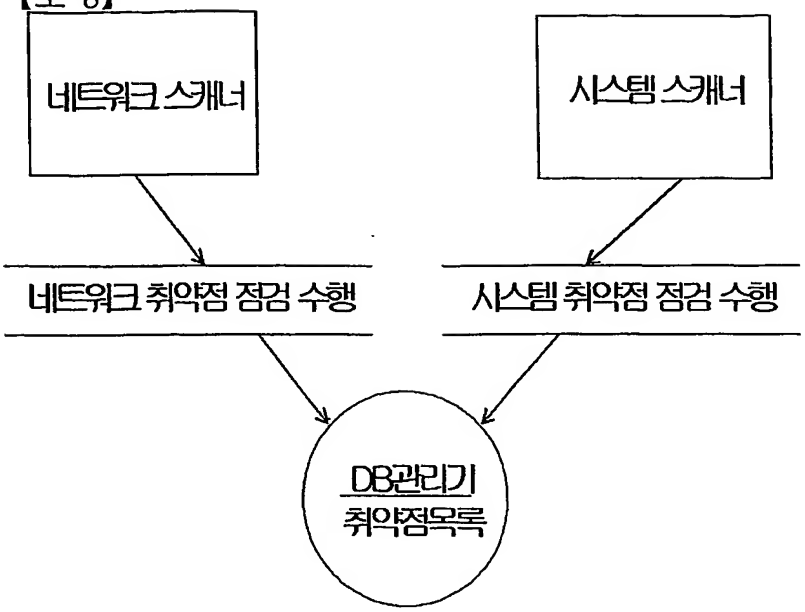
【도 6】


취약점 목록
스케너 결과
취약점 점검 결과
최신 바이러스 자료
정보수집 체계
보안기술자료
침해사고 정보
시스템 프로파일 정보
통합 보안 이벤트

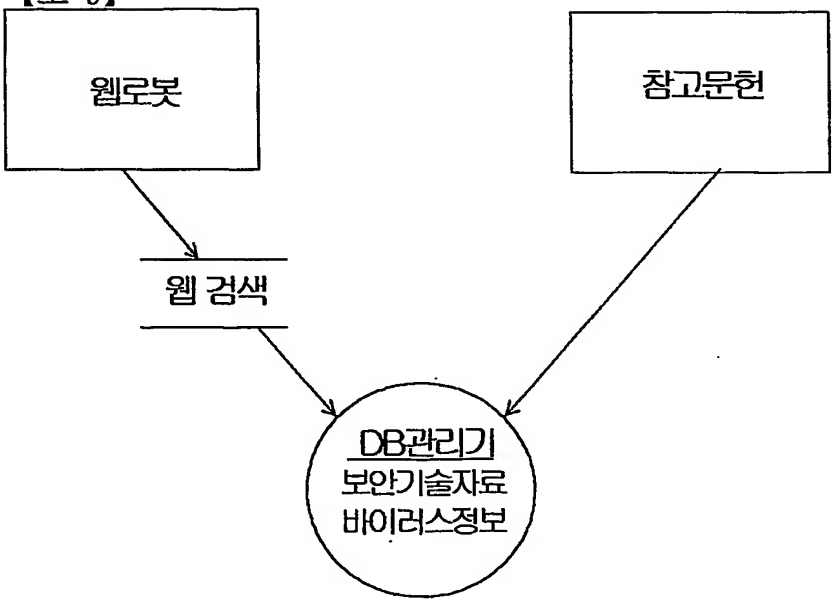
【도 7】


하드웨어 제작사
- 일반정보
- Patch정보
운영체제 제작사
- 버전정보
- Patch정보
- 취약점(문제점)/대책
DB관리기
취약점목록
어플리케이션 제작사
- 버전정보
- Patch정보
취약점(문제점)/대책
국내외 정보수집기관
- CVE/CAN 정보
- Bugtrack

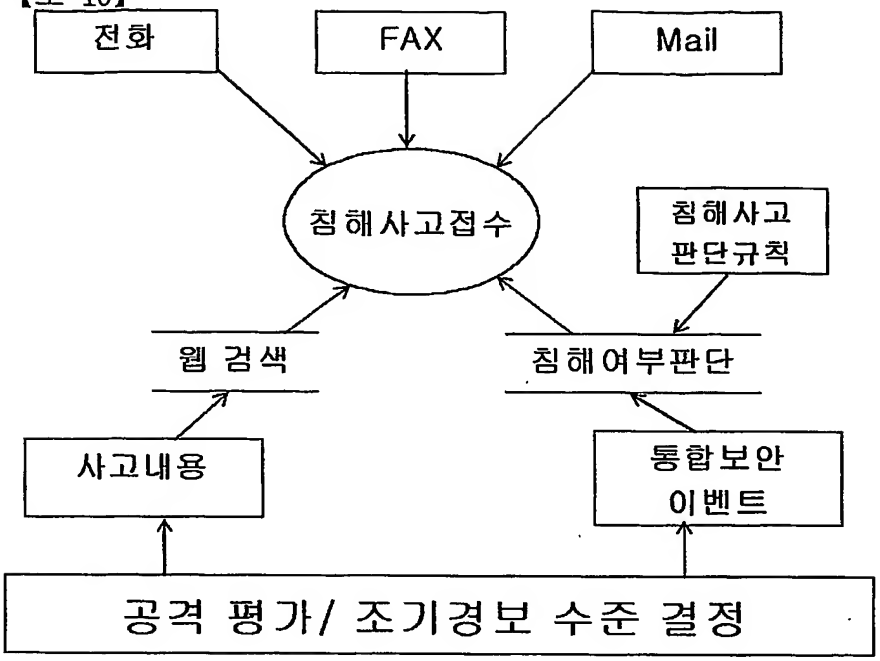
【도 8】


네트워크 스캐너
시스템 스캐너
네트워크 취약점 점검 수행
시스템 취약점 점검 수행
DB관리기
취약점목록

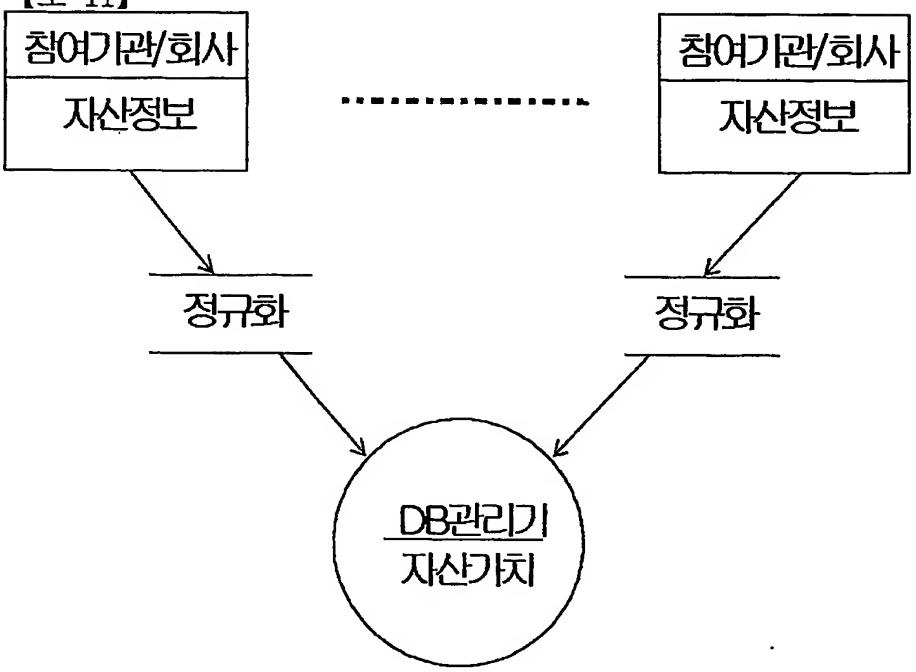
【도 9】


웹로봇
참고문헌
웹 검색
DB관리기
보안기술자료
바이러스정보

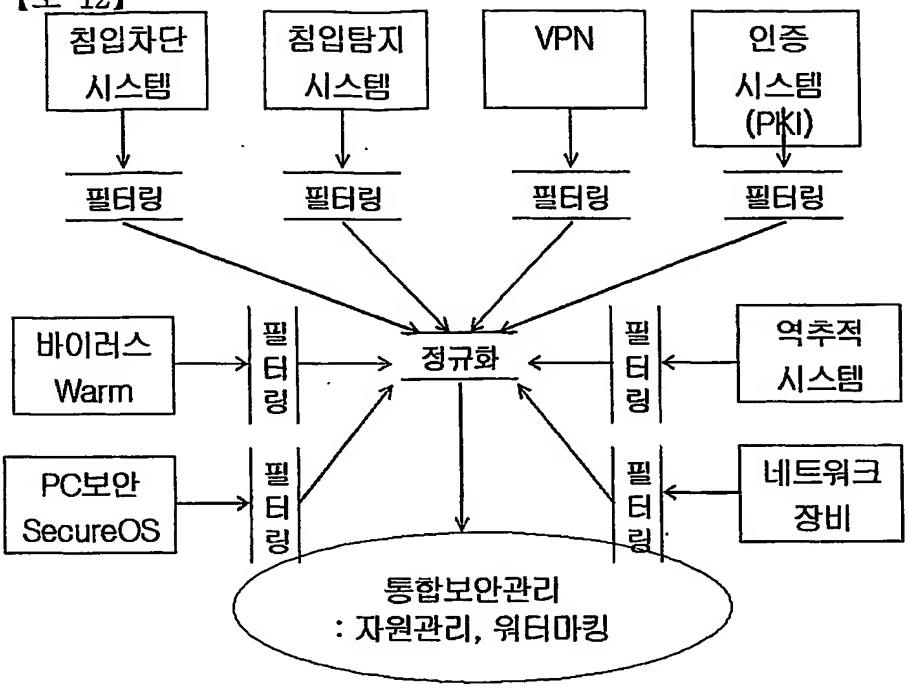
【도 10】


전화
FAX
Mail
침해사고접수
침해사고
판단규칙
웹 검색
침해여부판단
사고내용
통합보안
이벤트
공격 평가/ 조기경보 수준 결정

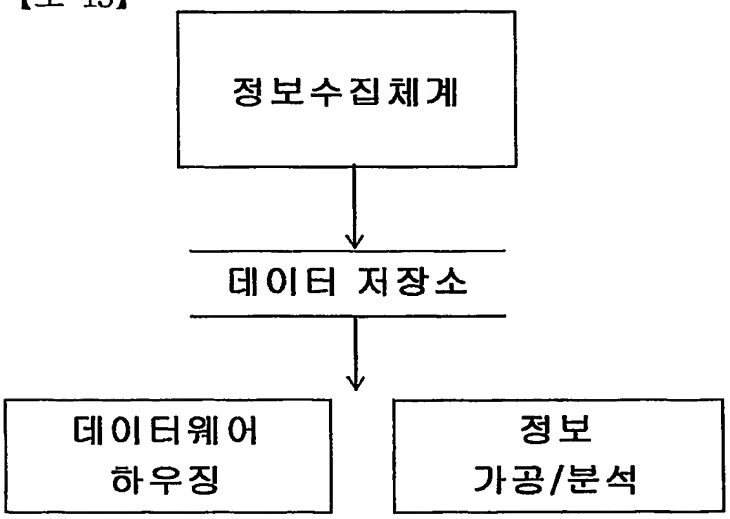
【도 11】


참여기관/회사
자산정보
참여기관/회사
자산정보
정규화
정규화
DB관리기
자산가치

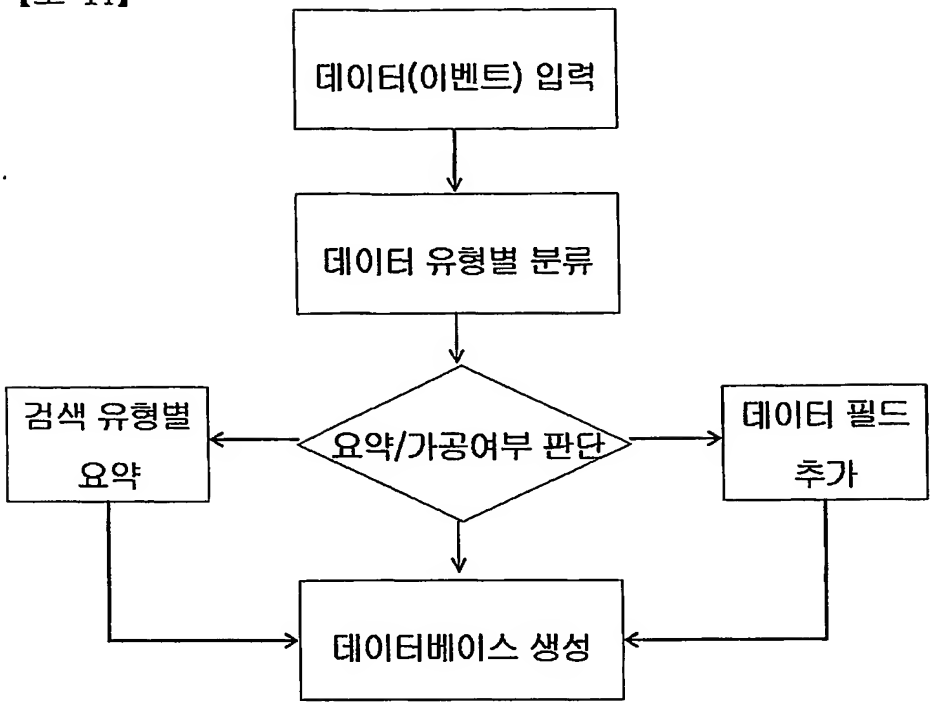
【도 12】


침입차단 시스템
침입탐지 시스템
VPN
인증 시스템 (PKI)
필터링
필터링
필터링
필터링
바이러스 Warm
필터링
정규화
필터링
역추적 시스템
PC보안 SecureOS
필터링
필터링
네트워크 장비
통합보안관리
: 자원관리, 워터마킹

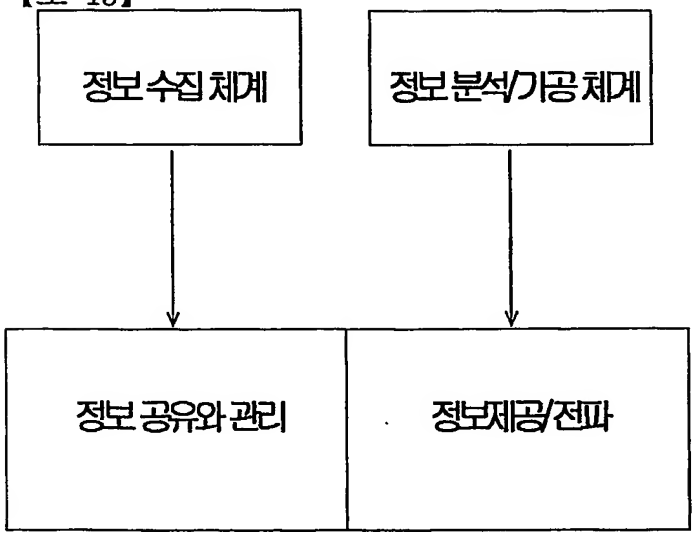
【도 13】


정보수집체계
데이터 저장소
데이터웨어 하우징
정보 가공/분석

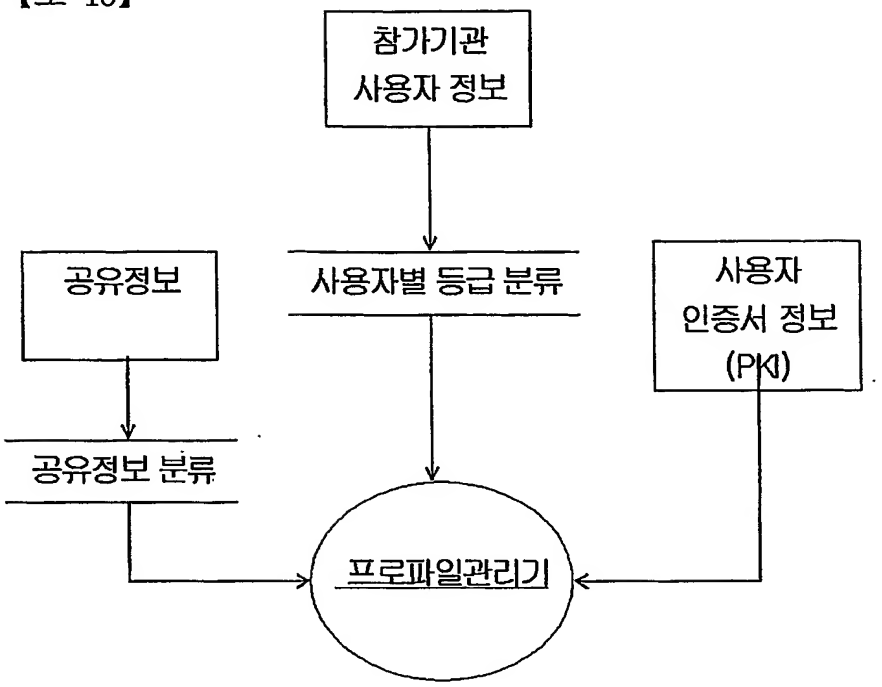
【도 14】


데이터(이벤트) 입력
데이터 유형별 분류
요약/가공여부 판단
검색 유형별 요약
데이터 필드 추가
데이터베이스 생성

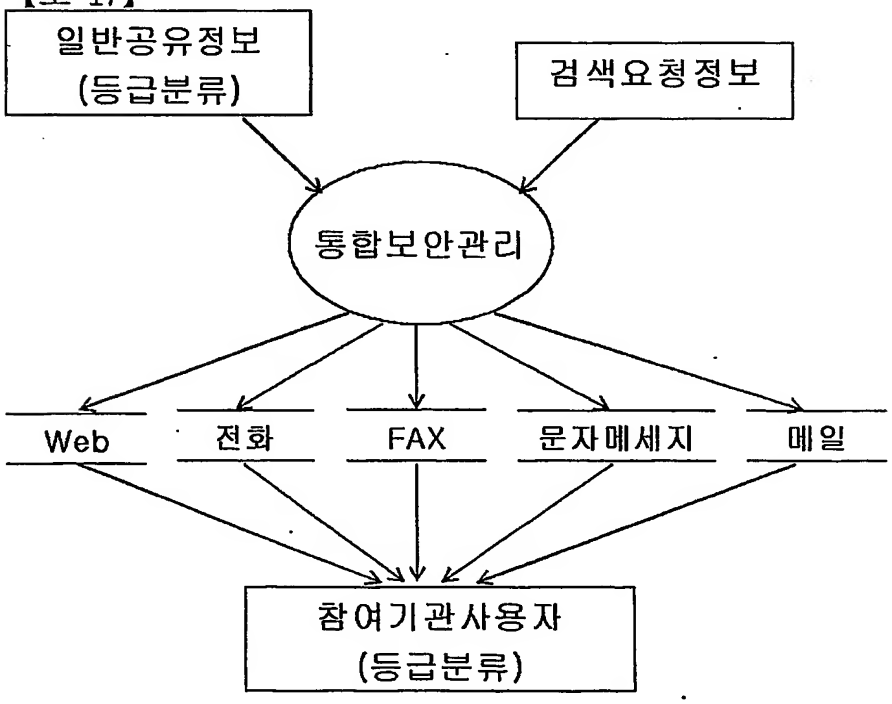
【도 15】


정보 수집 체계
정보 분석/가공 체계
정보 공유와 관리
정보제공/전파

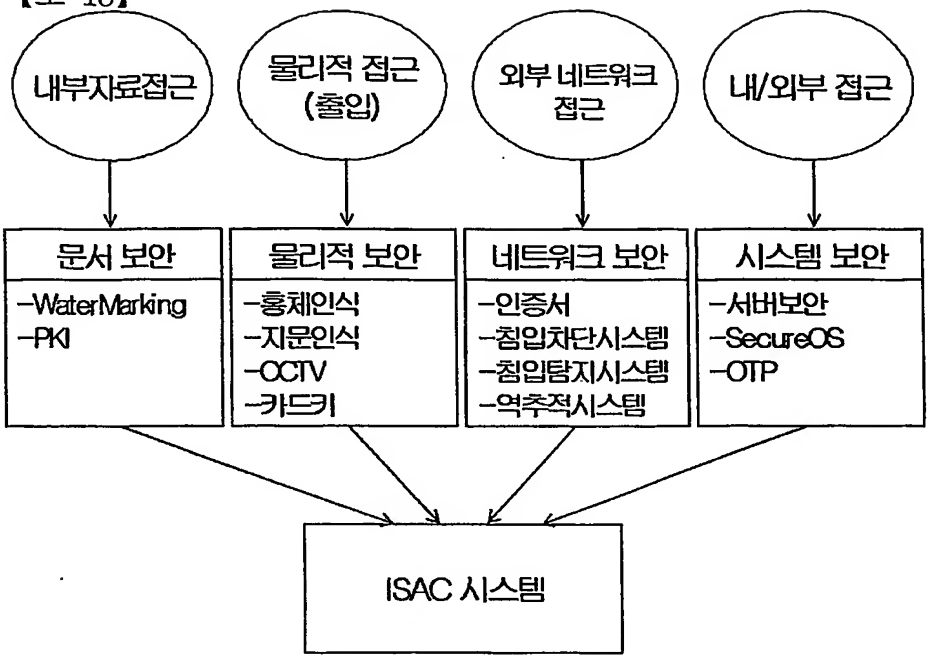
【도 16】


참가기관
사용자 정보
공유정보
사용자별 등급 분류
사용자
인증서 정보
(PKI)
공유정보 분류
프로파일관리기

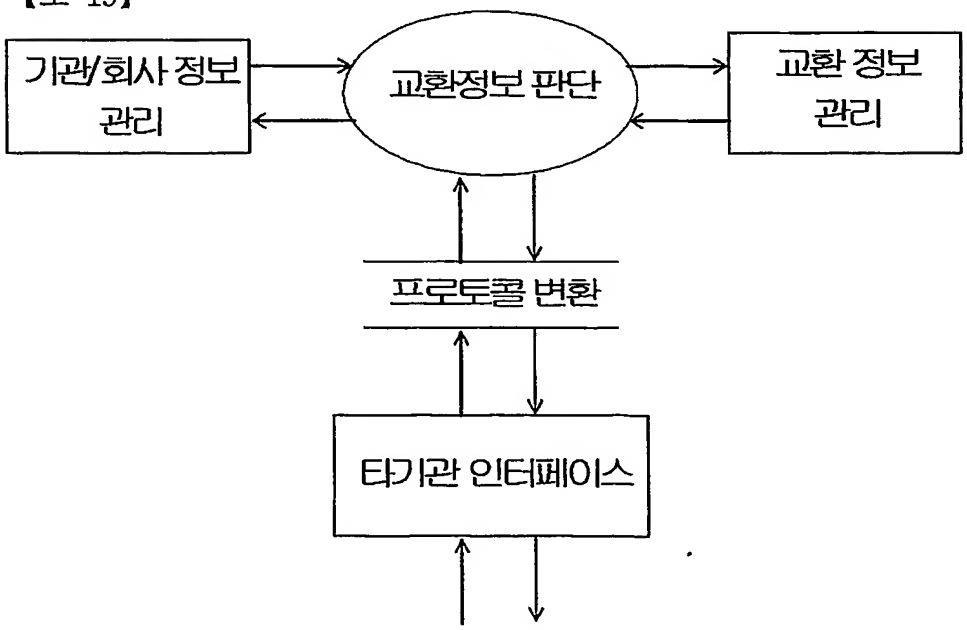
【도 17】


일반공유정보
(등급분류)
검색요청정보
통합보안관리
Web
전화
FAX
문자메세지
메일
참여기관사용자
(등급분류)

【도 18】


내부자료접근
물리적 접근 (출입)
외부 네트워크 접근
내/외부 접근
문서 보안
-WaterMarking
-PKI
물리적 보안
-홍체인식
-지문인식
-CCTV
-카드키
네트워크 보안
-인증서
-침입차단시스템
-침입탐지시스템
-역추적시스템
시스템 보안
-서버보안
-SecureOS
-OTP
ISAC 시스템

【도 19】


기관/회사 정보 관리
교환정보 판단
교환 정보 관리
프로토콜 변환
타기관 인터페이스